

Form Approved  
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE 22 MAY 97	3. REPORT TYPE AND DATES COVERED MONOGRAPH
----------------------------------	-----------------------------	---

### 5. FUNDING NUMBERS

**8. PERFORMING ORGANIZATION  
REPORT NUMBER**

**10. SPONSORING / MONITORING  
AGENCY REPORT NUMBER**

12b. DISTRIBUTION CODE

19971106 158

16. PRICE CODE

20. LIMITATION OF ABSTRACT  
UNLIMITED

# **PROTECTION AGAINST TERRORISM: DOES THE 1998 FM 100-5 SAY ENOUGH**

**A MONOGRAPH  
BY  
Major Thomas E. Bryant  
Signal Corps**



**School of Advanced Military Studies  
United States Army Command and General Staff  
College  
Fort Leavenworth, Kansas**

**SECOND TERM AY 96-97**

Approved for Public Release Distribution is Unlimited


SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

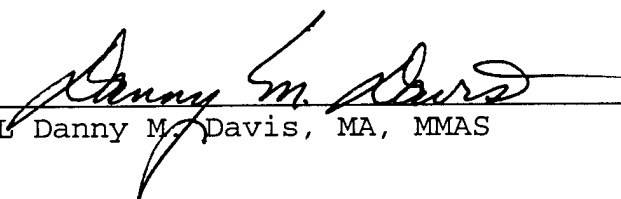
Major Thomas E. Bryant

Title of Monograph: *Protection Against Terrorism: Does the 1998  
FM 100-5 Say Enough?*

Approved by:

  
\_\_\_\_\_  
LTC Michael L. Parker, MMAS

Monograph Director

  
\_\_\_\_\_  
COL Danny M. Davis, MA, MMAS

Director, School of  
Advanced Military  
Studies

  
\_\_\_\_\_  
Philip J. Brookes, Ph.D.

Director, Graduate  
Degree Program

Accepted this 22d Day of May 1997

***Protection Against Terrorism:***  
***Does the 1998 FM 100-5 Say Enough?***

A Monograph  
By  
Major Thomas E. Bryant  
Signal Corps

School Of Advanced Military Studies  
United States Army Command And General Staff College  
Fort Leavenworth, Kansas

Term Two AY 96-97

## ABSTRACT

PROTECTION AGAINST TERRORISM: DOES THE 1998 FM 100-5 SAY ENOUGH? by MAJ Thomas E. Bryant, USA, 71 pages.

This monograph examines the U.S. Army Draft 1998 Field Manual 100-5 *Operations* to determine whether the terrorist threat is sufficiently addressed to carry the Army into the 21st Century. First, this monograph shows the purpose of *Operations* as the Army's capstone manual and shows the importance of terrorism at the operational level of war because of the will of the American people. Second, it uses case studies from Beirut and Saudi Arabia to show how U.S. policy can be affected by terrorism, and to determine what weaknesses were found at the operational level of war by the Secretary of Defense directed investigations into those incidents. Third, the monograph used the DOD Combating Terrorism Program Handbook to establish criteria with which to evaluate the new *Operations*.

This monograph found that while the 1998 FM 100-5 *Operations* did address the terrorist threat, it did not adequately address the threat across the spectrum of conflict to give the operational commander a proper focus in force protection. The monograph concludes with a recommendation for changes and additions to be made to *Operations*.

## **SECTION I - INTRODUCTION**

Currently the U.S. Military is regarded as the most formidable military in the World. Few nations, if any, would want to face the U.S. on the conventional battlefield. As a result of this imbalance of power, many will choose not to face the military on the conventional battlefield, but to attack U.S. Military Forces through the use of terrorism on a battlefield which is difficult to define.

The Cold War is over and the U.S. Army is no longer posturing to face a large conventional threat. Post-Cold War operations have been on the low intensity side of the scale of conflict. While these low intensity conflicts, or Peace Operations, do not pose the danger of the conventional battlefield, they have placed the Army in positions where there is no clear delineation of sides; the good guys look just like the enemy. Because of the confusion of these conflicts and the fact that the U.S. Army has an overwhelming military advantage, these environments make the Army a lucrative target for terrorist attacks from those who do not agree with U.S. policy and cannot face the Army in a direct confrontation.

During these less intensive conflicts, the will of the American people has been a pivotal key to the successful completion of these operations which may have had a national objective that was less than obvious to the populace and not directly linked to U.S. National Survival. Without the will of the American people, the Government, and thus the Military, cannot accomplish the policy goals of the Administration and will ultimately fail in its military mission.

The U.S. military has been on the receiving end of several acts of terrorism in the last fifteen years. The two most notable were the bombing of the Marine barracks in Beirut, Lebanon in 1983 and the 1996 attack on the Air Force barracks in Dhahran, Saudi Arabia. These examples show that Force Protection at the Operational Level of War against the terrorist threat is vital to the accomplishment of the Military's mission and attaining the Strategic Objectives.

Although the Army has not been targeted by such a catastrophic attack, it would do well to learn from the misfortunes of the Marine Corps and the Air Force. The 1998 FM 100-5 *Operations* will be a great opportunity to insure that the proper emphasis is placed on the subject of terrorism. Additionally, it is imperative that Army Doctrine links its concept of terrorist protection with Joint Doctrine so as to insure a unity of effort throughout the services.

## **U.S. ARMY DOCTRINE**

U.S. Army doctrine is designed to provide descriptive and prescriptive guidance by which Army forces guide their actions in support of national objectives; it is a guide for action to be applied with judgment. It thereby sets a standard of commonality for the planning and conduct of Army actions during joint, multinational, and interagency operations. FM 100-5 *Operations* is the U.S. Army's keystone operational doctrine manual and "provides guidance for the use of the Army in the service of national objectives and establishes the basis for subordinate Army doctrine, organization, training, material, leader and soldier development".<sup>1</sup>

## **PURPOSE OF FM 100-5**

FM 100-5 *Operations* is first and foremost a warfighting manual. It is the Army's keystone warfighting manual. FM 100-5 has a dual focus. First, it describes the operational art as the linkage of the tactical means to the strategic ends. Second, it describes how we fight -- the "art of operations" that includes fundamental tactical principles and forms of maneuver. It is a comprehensive description of how Army forces plan and execute campaigns, major operations, battles, and engagements.<sup>2</sup>

The 1998 FM 100-5 is the 14th in a series that began in 1905 and the second to be published since the end of the Cold War. Its goal is to address the full range of operations that the Army expects to execute in the foreseeable future -- offensive, defensive, stability and support operations.<sup>3</sup>

The 1998 FM 100-5 *Operations* is not intended to be a manual that focuses on the terrorist threat. However, because of the nature of the manual and its ability to focus the attention of the operational commanders and staffs and to shape the doctrine that is written in the future, it must address the terrorist threat in sufficient detail to insure that those faced with the threat will be aware of its significance.

## **OPERATIONAL LEVEL OF WAR**

There are three levels of war; strategic, operational, and tactical. These levels of war are "doctrinal perspectives that clarify the links between strategic objectives and tactical actions".<sup>4</sup> There are no definitive, clear cut boundaries between the levels of war but they are typically determined by their effect in achieving strategic, operational or tactical objectives.<sup>5</sup> The levels of war apply to all points on the scale of conflict.<sup>6</sup>



As a result of advances in technology, particularly communications and the media, the levels of war have a growing relationship and a single event can cut across all the levels. Due to this interrelationship, commanders at all levels must understand and account for how actions at one level may affect actions or reactions at the other levels.<sup>7</sup>

The strategic level of war is that level which a nation determines national strategic security objectives and guidance and uses national resources to meet its objectives.<sup>8</sup>

Strategy is therefore the “art and science of developing and employing armed forces and other national power in a synchronized fashion to secure national ... objectives”.<sup>9</sup> The strategy, derived from policy objectives is the basis for all operations.<sup>10</sup>

The tactical level of war is the “employment of units in combat”.<sup>11</sup> It is the placement of maneuver units in relation to each other and the enemy in order to use their full potential to attain the tactical objective.<sup>12</sup> Tactics are employed in engagements, which are short duration conflict fought between small forces and battles, which consist of a set of related engagements.<sup>13</sup> The summation of these engagements could affect the course of a campaign.

The operational level of war is the element that links strategy to tactics. The main focus at the operational level is on operational art. Operational art is the “use of military forces to achieve strategic goals through the design, organization integration, and conduct of strategies, campaigns major operations, and battles”.<sup>14</sup>

Operational art is the tool that allows commanders use their resources efficiently and effectively to achieve strategic objectives. It provides a framework that allows

commanders and staffs to understand the conditions for victory before battle and avoid unnecessary battles.<sup>15</sup>

There are many considerations which the operational commander must make. First, he must consider his Ends, which are the military conditions he must produce in order to achieve his strategic goal. Second, he must consider his Ways, which are the sequence of actions that are most likely to produce his desired Ends. Third, he must consider his Means, which is the resources he has to accomplish the sequence of actions designated in Ways. Lastly, the operational commander must consider the Risk involved in the sequence of actions chosen.<sup>16</sup> The risks involved in the operation is the focus of this monograph.

The threat of terrorism is a substantial risk to the operational commander. Because of the pivotal role that the operational commander plays in the accomplishment of National Strategic Objectives, a single terrorist act can very quickly, through the loss of the will of the American people, jeopardize the accomplishment of his Operational Objective. The operational commander must weigh this risk heavily.

## **THE WILL OF THE PEOPLE**

The will of the people is a mighty instrument in the formulation and sustainment of American policy. The affects of this “will” can best be described by applying the model of Carl Von Clausewitz’s “Paradoxical Trinity” as described in his military classic *On War*.

The elements of Clausewitz’s “paradoxical trinity” are passion, chance and policy. Clausewitz explained each of them as follows. First, passion is the “primordial violence,

hatred, and enmity”.<sup>17</sup> This first element of the trinity is used to refer to the people, which Clausewitz regarded as both passionate and irrational. Second is the “play of chance and probability within which the creative spirit is free to roam”.<sup>18</sup> The second element, which Clausewitz uses to refer to the army (or military in general today) which is primarily determined by the character of the commander and the army. Further, the Army is affected by the fog and friction of war from which the outcome can never be completely forecast. The third element is the “element of subordination, as an instrument of policy, which makes it subject to reason alone”.<sup>19</sup> This element refers to the government which is the administrator of the political aims and sets the policy of the nation.

Because of the character of the elements of the trinity, the relationship of the parts of the trinity may or may not act in the same direction or for the same goals which cause tension between the elements. As long as they exist with a tension between them, they each act as a system of checks and balances within the society that is held together by the information that each of them share. The key element that causes the trinity to work is information.

As a result of technology and the media, information flow is much faster in today’s society than when Clausewitz wrote over 160 years ago. Because information can be in the homes of the American public within a matter of minutes, the operational commander must be cognoscente of the impact that his actions, or inaction, can have on the policy objectives which he is charged to accomplish.

In today's world, the U.S. military is routinely involved in military operations which may involve National Interests but do not impact on National Survival. As a result, the value of these missions is not always readily apparent to the American populace and can be quickly questioned. An act of terrorism conducted against a military unit can immediately sway the American people as to their support of a U.S. policy. The result of lack of attention to the terrorist threat by the Operational Commander can not only cause the loss of many soldiers lives, it can undermine the very mission that he is to pursue. The ultimate result: Military Failure.

#### **COMMANDER'S RESPONSIBILITY**

It is apparent to most military personnel that the commander is responsible for everything that happens or fails to happen within his command. Just as the commander is responsible for a military action that succeeds or fails to achieve its military objective, in the *Report of the DOD Commission on Beirut International Airport Terrorist Act, October 23, 1983*, the Long Commission found that the commander was responsible for the failure to protect his Marines from the terrorist attack that occurred in October 1983 even though the Commission also found that he was inadequately staffed and supported to counter the terrorist threat.<sup>20</sup> Likewise, in *Force Protection Assessment of USCENTCOM AOR and Khobar Towers, Report of the Downing Assessment Task Force*, the Downing Task Force found that the Air Force commander on the scene did "not do enough" to protect the lives of the Air Force personnel under his charge<sup>21</sup> prior to the Saudi Arabia bombing in June 1996.

The same is true today. Regardless of the political or strategic implications that may result from a terrorist attack, the commander is responsible for the safeguard of his subordinates, in spite of the other missions or situations that may seem more pressing or important.

## **PRINCIPLE RESEARCH QUESTION**

As the Army transitions into the 21st Century it must develop doctrine that will be adequate to not only “win the Nations wars”, but one which will protect the American soldier and the Policies which it is to implement. In order to do this, the 1998 FM 100-5 *Operations* must adequately address the terrorist threat.

The principle research question of this monograph will be: “Does The 1998 FM 100-5 Adequately Address Terrorism at the Operational Level of War for the Army of the 21st Century?”

## **LIMITATIONS**

This monograph will focus on the threat of a physical attack by a terrorist against an Army organization, facility or person. While the monograph recognizes that modern terrorists can attack information systems of the Army and cause massive damage to Army operations, information warfare will not be addressed. While no less dangerous to military operations, it may or may not immediately affect the will of the people and undermine National Policy.

## **MONOGRAPH METHODOLOGY**

The methodology of this monograph will initially be to describe the Operational Level of War to show its importance in accomplishing strategic objectives; describe the

nature and purpose of the new FM 100-5; explain how the will of the people can influence the military's mission success; and use Joint references to define the key terms and concepts which are applicable to terrorism so as to have an agreed-upon set of definitions and provide a common understanding of the terrorist threat. Second, the monograph will review the significance terrorist acts against U.S. Military targets has had on United States' policy through historical case studies. The case studies selected, Beirut and Saudi Arabia, will show the significance of terrorism to the Army and why terrorism is worthy of consideration by the Operational Commander. Third, the monograph will use Department of Defense Directive 0-2000.12-H, *Protection of DOD Personnel and Activities Against Acts of Terrorism and Public Turbulence* to establish a baseline from which to evaluate the Draft FM 100-5. This document will serve to determine the current strengths and shortfalls of the Draft FM 100-5 as it addresses the terrorist threat. Fourth, the monograph will review the considerations of the terrorist threat already made in the Draft FM 100-5 to assess whether it is adequate as it is currently written. Finally, the monograph will analyze the conclusions of the previous four sections to determine whether the 1998 FM 100-5 adequately addresses the terrorist threat in support of the operational commander and will make recommendations as to what action, if any, the Army should take to improve the Draft FM 100-5 *Operations*.

## **DEFINITIONS AND KEY TERMINOLOGY**

Force protection, terrorism, anti-terrorism and other associated terms are commonly misused and misunderstood among civilians, the media, as well as military

personnel. Due to the nature and purpose of this monograph, Department of Defense definitions will be used, where possible, in order to provide an agreed upon reference set.

Force Protection is defined as “a security program designed to protect soldiers, civilian employees, family members, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, personal protective services, and supported by intelligence, counterintelligence, and other security programs.”<sup>22</sup>

Unconventional Warfare (UW) is defined as “a broad spectrum of military and paramilitary operations conducted in enemy-held, enemy-controlled, or politically sensitive territory. UW includes guerrilla warfare, evasion and escape, subversion, sabotage, direct action missions, and other operations of low visibility, covert, or clandestine nature. These interrelated aspects of UW may be prosecuted singly or collectively by predominately indigenous personnel, usually supported and directed in varying degrees by an external source during all conditions of war or peace.”<sup>23</sup>

Terrorism is defined as the “calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.”<sup>24</sup> Although not specifically stated as such, terrorism is sub-set of Unconventional Warfare.

Political terrorism is the “use or threat of use, of violence, by an individual or group, whether acting for or in opposition to established authority, when such action is designed to create extreme anxiety and /or fear-inducing effects in a target group larger

than the immediate victims with the purpose of coercing that group into conceding to the political demands of the perpetrators.”<sup>25</sup>

Counterterrorism is the “offensive measures taken to prevent, deter and respond to terrorism.”<sup>26</sup> U.S. counterterrorism programs are classified.<sup>27</sup>

Antiterrorism is the “defensive measures to reduce the vulnerability of individuals and property to terrorists acts, to include limited response and containment by local military forces.”<sup>28</sup>

Antiterrorism Awareness is the “fundamental knowledge of the terrorist threat and measures to reduce vulnerability to terrorism.”<sup>29</sup> Antiterrorism Awareness is, in essence, situational awareness.

## **SECTION II - TERRORISM AND U.S. FOREIGN POLICY**

### **Introduction**

“Terrorists attack targets which are vulnerable, have high psychological impact on society, produce significant publicity”<sup>30</sup> and contribute to the perceived weakness of a nation.<sup>31</sup> As such, U.S. military forces make a lucrative target for terrorists interested in dictating U.S. foreign policy. In operations other than actual war, terrorist attacks against military targets are not military in nature. They are typically directed at the political policy of the target nation in an attempt to damage national prestige or posture or to sway the political decision making of that country.<sup>32</sup> It is not the actual attack on the military force that is the goal.



United States assets are targets of terrorism for a variety of reasons. Many nations and elements harbor animosity against the U.S. because of ideological differences, because the U.S. is a leading industrial power, or because the U.S. is a leading capitalist state. Another powerful reason to target U.S. assets with terrorism is that some perceive that the U.S. can dictate the actions of other independent nations due to its relative strength. Although the U.S. takes a hard line on terrorism, the reasons that make U.S. interests a target remain constant and real. Whatever the reason, U.S. personnel and interests provide a viable target because of their mere presence - U.S. personnel, especially U.S. Military personnel, are everywhere.<sup>33</sup>

## **Methodology**

This section will examine two case studies, the 1983 Beirut, Lebanon bombing and the 1996 Dhahran, Saudi Arabia bombing where U.S. military forces were targets of terrorist attack. In both cases the ultimate goal of the terrorists was the withdrawal of U.S. forces from the regions. This section will first serve to show the significance of the terrorist threat to the operational commander by an evaluation of the success of the attack on U.S. National Policy and second it will use the Secretary of Defense directed investigations into the incidents to determine where the actions of the operational commander were either incorrect or inadequate in the prevention of a terrorist attack.

To measure the success of the terrorist attacks this monograph will use the five major goals of terrorism as a framework to evaluate the strategic implications and the success of the attacks. The first major goal of terrorism is to publicize its cause among two distinct audiences; first, to the group which the group claims to represent and

second, the international community or portions of that community.<sup>34</sup> The second major goal of terrorism is to intimidate and harass authorities and to make life hard for them so as to force them to make concessions. The terrorist seeks to deprive the opposition of material resources, law and order, or piece of mind. This is called "coercive diplomacy".<sup>35</sup> The third major goal of terrorism is to force polarization of society, to disrupt the status quo.<sup>36</sup> The fourth major goal of terrorism is to aggravate relations between states so as to prevent a set of political events unfavorable to the terrorist group.<sup>37</sup> The fifth major goal of terrorism is the freeing of prisoners and the securing of monetary ransoms.<sup>38</sup>

To protect forces from the terrorist threat the operational level commander must understand the terrorist threat and provide guidance and support to subordinates to prevent attacks. To determine the shortcomings or inadequacies of the operational commander in these case studies this monograph will use the findings of the official investigations into the incidents. For the Beirut case study the monograph will use the *Report on the DOD Commission on Beirut International Airport Terrorist Act, October 23, 1983*. For the Saudi Arabia bombing the monograph will use the *Report of the Downing Assessment Task Force*.

The section will conclude with an analysis of the significance of the terrorist threat to the National Policy and the operational commander, of the similarities between the two attacks, and of what portions of the DOD Handbook should be used to evaluate the Draft FM 100-5 *Operations*.

## **BEIRUT CASE STUDY**

### **Background**

In the early 1980's Lebanon was a small weak nation in a region of great tension and conflict "beset with virtually every unresolved dispute afflicting the peoples of the Middle East". The Government of Lebanon was a "creature of confessionalism and localism", which is to say that it was made deliberately weak to accommodate the different and diverse religious factions in the nation in an attempt to provide some type of government.<sup>39</sup> "Without consensus, any controversial stand taken by the central government would be labeled as ... favoritism by those who opposed it."<sup>40</sup> The country of Lebanon was basically a battleground for Syrians and the Israelis to conduct an indirect war with each other; in essence, Lebanon had become a battleground where armed Lebanese factions simultaneously manipulated and were manipulated by the foreign forces around them.<sup>41</sup>

The United States became involved in Lebanon in mid-1982. On 6 June of that year the Israeli Defense Force (IDF), in an effort to destroy Palestine Liberation Organization (PLO) elements, invaded Lebanon and within three days had rolled-up the PLO from the Israeli-Lebanese border to the outskirts of the capital of Beirut.<sup>42</sup> In response, the U.S. positioned a Marine Amphibious Unit (MAU) off the coast of Lebanon to protect U.S. citizens. On 23 June 1982 the MAU conducted a successful non-combatant evacuation operation (NEO) of U.S. citizens from the port of city of Joniyah.<sup>43</sup>

On 2 July 1982, the IDF instituted a blockade of the capitol city of Beirut. As a result, a Multi-National Force (MNF) was formed consisting of French and Italian forces

and the MAU. This MNF evacuated some 15,000 armed Palestinians and Syrians from Beirut to prevent the IDF from destroying the city with a military attack. The MNF completed its mission successfully and was withdrawn by 10 September 1982.<sup>44</sup>

Within a week, events in Lebanon escalated. On 14 September the Lebanese President-elect Bachir Gemaer was assassinated and Christian - IDF forces massacred some 800 Palestinian and Lebanese civilians in refugee camps. These actions brought about the reconstitution of the MNF. By 29 September the MNF had reentered Beirut.<sup>45</sup>

As part of the MNF, the mission of the MAU (USMNF) was "to establish an environment that would facilitate the withdrawal of foreign military forces from Lebanon and to assist the Lebanese Government and the Lebanese Armed Forces in establishing sovereignty and authority over the Beirut area."<sup>46</sup> The U.S. government believed that the USMNF would be received among the Lebanese factions as "even-handed and neutral". This perception was accurate as the MAU was warmly welcomed and seemed to be appreciated by most Lebanese.<sup>47</sup> The operation was to be of short duration.<sup>48</sup>

As part of the MNF the MAU was assigned the sector of the Beirut International Airport (BIA). The BIA was strategically important because if the BIA remained open it signaled to the rest of the World that Lebanon was a functioning country.<sup>49</sup> As important, it signaled to the American people that the policy objectives of the Administration were succeeding. For security reasons this arrangement was unwise because it meant that the Marines would have to co-exist with civilians operating and flowing through the BIA. However, in light of the initial warm reception of the Marines by the local population, this policy was accepted.

By March 1983, the friendly environment began to deteriorate. A USMNF patrol was attacked by a hand grenade wounding five Marines; both the French and Italian MNF forces had similar incidents. The most significant indicator of the change in environment, however, was the 18 April bombing of the U.S. Embassy. The explosion destroyed the Embassy, killing 17 Americans and 60 others. The method of attack was a light truck packed with a "gas enhanced" explosive that produced an unprecedented explosion.<sup>50</sup>

During this period the mission of the Marines also escalated. They began providing training, ammunition resupply and naval gunfire to the LAF. These additional tasks expanded beyond their original peacekeeping mission and represented a shift from their initial neutrality. Although this increasing shift from their initial neutrality may have gone overlooked by the USMNF and its operational chain of command, it did not escape the rival factional militias in Lebanon. The image of the USMNF became pro-Israel, anti-Muslim, and a significant portion of the Lebanese populace no longer considered the USMNF as neutral.<sup>51</sup>

From April until October hostile incidents directed at the USMNF increased and in late July the BIA began receiving unintentional shelling from clashes between the LAF and factional militias. By early August, the USMNF received the first intentional shelling from factional forces.<sup>52</sup> From 14-16 October, two Marines were killed on the BIA perimeter in sniper incidents.<sup>53</sup> On 19 October, four Marines were wounded when a MAU convoy was attacked by a car bomb.<sup>54</sup> By the end of October the situation in Lebanon had clearly turned hostile to the USMNF, and as a result, the Marines

consolidated their positions in the USMNF headquarters building in an attempt to provide protection from sniper and indirect weapons fire.<sup>55</sup>

### **The Event - Bombing of the USMNF Barracks**

On 23 October 1983, the hostilities toward the MNF reached their zenith. At 05:00 A.M. that morning a guard post sentry spotted suspicious activity by a yellow Mercedes Benz truck in a parking lot near the USMNF headquarters, but did not report the incident because the truck did not park.<sup>56</sup> At approximately 06:22 A.M., a large yellow Mercedes-Benz stakebed truck containing over 12,000 pounds of TNT crashed the gate of the BIA, "drove over barbed wire, between two checkpoints (without being engaged), entered an open gate, passed around a barrier, flattened the sergeant of the guards booth and penetrated the lobby of the MAU headquarters and exploded."<sup>57</sup> As a result of the blast the building was destroyed and 241 Marines were killed with over 100 wounded. The truck spotted at 05:00 is believed to be the same one used during the attack at 06:22 A.M. Almost simultaneously with the attack on the USMNF, another, similar truck bomb exploded at the French MNF Headquarters.<sup>58</sup>

### **Strategic Implications**

Using the framework of the major goals of terrorists, this attack was an overwhelming success. To the first major goal of terrorism, publicity, the attack was a major success. The event received great publicity where it mattered - the U.S. The real target of the attack was the U.S. Congress and the American people.<sup>59</sup> The Lebanese terrorists had followed the public debates in the U.S. concerning the Marine deployment

to Beirut and understood that a lot of casualties would undermine the weak legislative support for the administration.<sup>60</sup>

To the second major goal of terrorism, intimidation and harassment of authorities and to make life hard for them so as to force them to make concessions, the attack was also a success. This “coercive diplomacy” caused U.S. President Ronald Reagan to announce the redeployment of the Marines to ships off the coast of Lebanon on 8 February 1984<sup>61</sup>, three months after the attack. The terrorist's strategy to generate enough casualties to persuade the U.S. led MNF to withdraw from Lebanon<sup>62</sup> was successful.

The last three major goals of terrorism are not relevant in the Beirut case study as the ultimate goal was achieved by the first two and there were no hostages involved. The Presidents’ decision to pull the Marines from Lebanon resulted primarily from Congressional disapproval, inability of the Administration to articulate a consistent policy, and the fact that 1984 was an election year.<sup>63</sup> The withdrawal of the Marines from Lebanon is one of the most impressive examples of terrorist influence on government policy.<sup>64</sup>

### **Operational Findings**

Following the bombing, the Secretary of Defense convened the DOD Commission on Beirut International Airport (BIA) Terrorist Act of October 23, 1983 (Long Commission) to investigate the incident. The Commission made several findings that are relevant to the operational commander.

First, the Long Commission found that the USMNF was not trained, organized, staffed or supported to deal with the terrorist threat in Lebanon.<sup>65</sup> As a result, the

USMNF commander was unable to process or act upon the more than 100 intelligence reports warning of terrorist carbomb attacks received between May 1983 and November 1983.<sup>66</sup> This inability to understand the terrorist threat led the USMNF commander to place his forces in one central location; to this, the Long Commission determined that putting so many of the forces in one location made it a lucrative terrorist target.<sup>67</sup>

Second, the Commission found that the operational chain of command<sup>68</sup> did not understand the terrorist threat to the USMNF, although the recent events and intelligence reporting provided adequate warning. This is underscored by the fact that the USEUCOM Special Assistant for Security Matters(SASM), who had specific responsibility for analyzing security against terrorist attacks, visited the Beirut Office of Military Cooperation(OMC) following the U.S. Embassy bombing and initiated a number of antiterrorism measures at the OMC during the visit. The SASM team was not charged by USCINCEUR to evaluate the antiterrorism defenses of the USMNF and did not do so.<sup>69</sup> Additionally, principle and senior staff officers within the operational chain of command visited the USMNF at the BIA prior to the 23 October bombing and the Long Commission found no evidence that they made any recommended security changes.<sup>70</sup>

The Long Commission's inquiry further showed that the attitude of the operational chain of command was that the security measures in effect were the "sole province" of the USMNF commander, and that it would be improper to tell him how to best protect his forces.<sup>71</sup> "Each level in the chain of command recognized that the environment in which the USMNF was operating changed from a generally benign to



increasingly hostile through the spring and summer of 1983.”<sup>72</sup> Neither the mission nor security measures, however, were changed.<sup>73</sup>

Third, although it was clear that the USMNF was not prepared for such an attack due to inadequate staffing, procedures and changes in environment compared to the mission, the Long Commission held that “military commanders are responsible for the security of their subordinates”.<sup>74</sup> The Commission further recommended that the “Secretary of Defense take whatever... action he deems appropriate, citing failure of the USCINCEUR *operational chain of command* to monitor and supervise effectively the security measures and procedures employed by the USMNF on 23 October 1983.”<sup>75</sup> (Italics added.)

### **Conclusions - Beirut**

The mission of the USMNF was one of Peace Enforcement. Therefore the terrorist attack was not military in nature because the Marines were not combatants.<sup>76</sup> Those who perpetrated the attack against the Americans and Western presence in Lebanon understood that the battleground was not in Lebanon, but in the United States<sup>77</sup>, a point which the operational commanders failed to understand or prepare for. The operational commanders failed to understand the threat, act to protect the USMNF or provide adequate staffing and support to the USMNF so that it could protect itself. The operational commanders failed to act. As a result of the lack of attention to Force Protection at the operational level, the military mission, and the U.S. National Policy in Lebanon failed.

## **SAUDI ARABIA CASE STUDY**

### **Background**

Prior to the 2 August 1990 attack into Kuwait by Iraq, the U.S. was generally welcomed by Saudi Arabia, but the U.S. presence was preferred to be “over the horizon.” Thus, most of the U.S. military presence was through the Middle East Force operating in the Arabian Gulf.<sup>78</sup>

After the Iraqi invasion of Kuwait, the U.S. led a coalition of Western and Islamic forces to defend Saudi Arabia, as well as other smaller Gulf states, and to free Kuwait from Iraq’s occupation. During Operation Desert Storm the coalition won an impressive military victory over Iraq, but not all of the threats to the region were removed.<sup>79</sup> In addition to the freeing of Kuwait, the U.S. vital interests of protecting the vast energy resources in the Gulf region remained.

Although the Iraqi Army was forced out of Kuwait during Operation Desert Storm, Saddam Hussein remained in power as a threat to the Gulf region. To help deter further aggression by Hussein, the U.S. remained in Saudi Arabia to insure enforcement of United Nations (UN) resolutions imposed on Iraq. One part of the UN Resolutions was the establishment of a “no-fly zone” along the 32 degree parallel which prohibits Iraqi aircraft from threatening its neighbors to the south. This operation, known as Operation Southern Watch, is manned by nearly 5,000 United States Air Force personnel who conducted combat air missions from bases in Saudi Arabia and Kuwait to enforce the “no-fly zone” over Iraq.<sup>80</sup>

Until 1994, terrorism in Saudi Arabia was considered improbable.<sup>81</sup> Since then, however, Islamic fundamental forces from Iran and Iraq have changed the relative safety of that country. These forces clearly want the U.S. presence out of Saudi Arabia.<sup>82</sup> Additionally, since the Gulf War, westernization in the Saudi Kingdom has further inflamed fundamentalist issues and dissidents within Saudi Arabia itself and they are putting pressure on King Fahd to renounce western influence.<sup>83</sup> Some of those opposition forces have turned to terrorism.<sup>84</sup>

The first two terrorist attacks in Saudi Arabia directed against U.S. personnel occurred in February 1991. In the first incident, terrorists attacked a bus in Jeddah and wounded three U.S. Military personnel and a Saudi Guard.<sup>85</sup> The perpetrators of that attack were subsequently captured by Saudi officials and executed.<sup>86</sup> In the second incident that month, unknown persons dowsed a U.S. transport bus with kerosene.<sup>87</sup>

The next terrorist attack in the Saudi Kingdom occurred on 13 November 1995. The target of this attack was personnel from the Office of the Program Manager, Saudi Arabian National Guard (OPMSANG).<sup>88</sup> The attack occurred at 11:40 A.M. near a downtown Riyadh snack bar frequented by U.S. personnel of OPMSANG. In this attack the terrorists used a van packed with explosives that detonated outside the snack bar. The explosion killed five Americans and wounded 60 others.<sup>89</sup> Four Sunni Muslims were captured following the attack and later confessed to the bombings. They were beheaded on 31 May 1996.<sup>90</sup>

## **The Event - Khobar Towers Bombing**

The mission of the 4404th Air Wing (Provisional) is to “serve as the front line defense against possible Iraqi aggression. To enforce UN Security Council Resolutions 687, 688, and 949 and protect U.S. forces stationed in Kuwait, United Arab Emirate and Saudi Arabia.”<sup>91</sup> Members of the 4404th Air Wing (Provisional) were housed in the Khobar Towers. The facility housed approximately 3,000 U.S. military personnel, as well as military personnel from the United Kingdom, France and Saudi Arabia. It had been used to house the U.S. personnel since 1991<sup>92</sup> because of its convenient location and the fact that it was paid for by the Saudi Government.<sup>93</sup>

At approximately noon on 25 June 1996 a suspicious truck attempted to enter the compound but was turned away. Shortly before 10:00 P.M. a fuel truck approached the northern perimeter fence of the Khobar compound and parked. The driver left the vehicle and fled the area. Within a few minutes the truck exploded, destroying the building closest to the perimeter fence that housed U.S. Airmen. Nineteen U.S. Airmen were killed and 547 were injured in the blast.<sup>94</sup>

## **Strategic Implications**

The goal of the terrorist attack at Khobar Towers was to force the withdrawal of U.S. forces from Saudi Arabia and the Persian Gulf region.<sup>95</sup> Although the U.S. did not conduct the withdrawal that the terrorist hoped for, the attack was partially successful.

The first goal of terrorism is publicity.<sup>96</sup> To this goal the attack was successful. From the publicity there was the severe criticism of Secretary of Defense William Perry, CJCS General John Shalikashvili, the Department of Defense, and all leadership in the

chain of command. There was a general feeling of distrust for military leadership.<sup>97</sup>

Senator Strom Thurmon, chairman of the Senate Armed Services Committee, referring to previous attacks, summed up America's frustration and distrust saying, "Average Americans would think that we had learned something from these incidents about protecting our forces and progressed beyond the point at which we find ourselves today."<sup>98</sup>

The second major goal of terrorism is to intimidate and harass authorities so as to force them to make concessions and deprive them of resources and piece of mind.<sup>99</sup> To this goal also the attack was also a success. One concession was the almost immediate plan to move of U.S. forces to a secluded base sixty miles from Riyadh; a move that could easily be viewed as a retreat in the face of a terrorist threat. Further, the cost of moving the U.S. soldiers to a safer location is estimated to be \$200 million, which the U.S. and Saudi government have agreed to share.<sup>100</sup> It is also obvious that any piece of mind that the U.S. forces had about the security in Saudi Arabia was shattered in the attack.

The third major goal of terrorism, the polarization of society<sup>101</sup> was likely achieved to some degree within the Saudi Arabian society, although it is difficult to determine to what level.

The fourth major goal of terrorism is to "aggravate relations between states so as to prevent a set of political events unfavorable to the terrorist group."<sup>102</sup> To this goal the attack was successful. The attack placed a great deal of strain on the relationship between the U.S. and Saudi Arabia because the U.S. asserted that the Saudi government was

uncooperative in attempts to heighten security around the target and the U.S. instead demanded that the Federal Bureau of Investigation (FBI) be allowed to assist in the investigation. Coordinating civil and military affairs is extremely difficult with allies. The host nation has to remain the allegiance of its own population and not have the guest undermine the legitimacy of the host government.<sup>103</sup> The attack placed both governments in a precarious diplomatic situation.

The fifth goal of terrorism is not applicable as there were no prisoners to release.

### **Operational Findings**

Following the Khobar Towers attack, the Secretary of Defense convened the Downing Assessment Task Force to investigate the attack. The Downing Commission made 26 findings and 78 recommendations. Among them were five which, like the attack itself, were similar to the Beirut attack 13 years earlier and have implications for the operational commander.

The first was Finding 3 - *Joint Task Force Southeast Asia and other U.S. Central Command units in the region were not structured or supported to sustain long term commitment that involved expanded missions, to include increased force protection from an emerging and viable terrorist threat.*<sup>104</sup> The finding consisted of three major points: 1) there were too few people to increase THREATCON level to THREATCON CHARLIE, which was appropriate.<sup>105</sup>; 2) The tour of duty for personnel was too short for continuity.<sup>106</sup>; 3) The mission changed but the force structure to support changes did not.<sup>107</sup>

The second was Finding 6 - *There is no theater-specific training guidance for individuals or units deploying to the U.S. Central Command Area of Responsibility.*<sup>108</sup>

In this finding it was noted that some units and individuals had received antiterrorism training while others had not. Even among those who had, for example the antiterrorism officer at Khobar Towers, it had been five to ten years since the training.<sup>109</sup> There was no standard established for the AOR.

The third was Finding 7 - *Intelligence sources provided warning of the terrorist threat to U.S. forces in Saudi Arabia.*<sup>110</sup> The intelligence provided commanders warning in time and motivation to react to the terrorist threat and reduce vulnerabilities.<sup>111</sup> This is discussed further in Finding 20 below.

The fourth was Finding 18 - *Although intelligence did not provide the tactical details of date, time, place and exact method of attack on Khobar towers, a considerable body of information was available that indicated terrorists had the capability and intention to target U.S. interests and that Khobar Towers was a potential target.*<sup>112</sup>

Disturbing in this finding is that the Air Force Office of Special Investigations Detachment(OSID) sent a message to Headquarters, Air Force Office of Special Investigations in Washington, DC on 4 April 1996 identifying vulnerabilities concluding that the "security measures here are outstanding, which in my view would lead a would-be terrorist to attempt and attack from a position outside the perimeter"...and... "if a truck parks close to the fence line, and the driver makes a quick getaway, I think the building should be cleared immediately."<sup>113</sup>

The fifth finding was Finding 19 - *The chain of command did not provide adequate guidance and support to the Commander 4404th Air Wing (Provisional).*<sup>114</sup>

Two points are important. Conditions and circumstances created at all levels of the chain of command caused vulnerabilities that were exploited in the actual attack<sup>115</sup> and no member to the U.S. Air Forces Central Command chain of command inspected physical security at Khobar Towers.<sup>116</sup>

The last Finding was 20 - *The Commander, 4404th Air Wing (Provisional) did not adequately protect his forces.*<sup>117</sup> Khobar Towers was identified to the 4404th Commander, General Schwalier as one of the three highest priority soft targets in the region<sup>118</sup> and General Schwalier never raised to his superiors force protection matters that were beyond his capability to correct.<sup>119</sup>

### **Conclusions - Saudi Arabia**

Like the USMNF in Beirut, the 4404th Air Wing was not involved in combat. Those who perpetrated the attack had learned from the Gulf War that the U.S. could not be faced on the conventional battlefield so they resorted to terrorism. This was a tactic which the operational commanders were not prepared for. Although the ultimate goal of the terrorists, withdrawal of U.S. forces from the region was not achieved, there were many strategic implications from the attack. As a result of the lack of attention to Force Protection at the operational level, the U.S. National Policy in Saudi Arabia was weakened. Like the operational commanders in Beirut, the command was found at fault.



## SECTION II CONCLUSIONS

Today, the United States has the most powerful military in the world. Through these two case studies, however, it is evident that this overwhelming military advantage can be reduced by a terrorist act. Within four months of the attack on the U.S. Marines in Beirut the ultimate goal of the terrorist was achieved. The results of the terrorist attack in Dhahran were not as successful, but it did aggravate the U.S. - Saudi alliance, cost both governments millions of dollars, and shook the confidence of all U.S. forces deployed in the Middle East, if not the rest of the world. Worse yet, it undermined the American confidence in the Military leadership.

The findings of the Long Commission and the Downing Task Force are startlingly similar, yet 13 years apart. In both cases the operational commanders failed to adequately train and organize their forces, discern the terrorist threat, and failed to act to protect their forces from terrorist attack. In both cases the operational commanders were found at fault. As summed up by Senator Thurmond, the American people expect more from their military commanders. Lack of attention to the terrorist threat cost money, lives, policy and National prestige. To preclude a repeat of these incidents, Secretary of Defense Perry changed the scope of Department of Defense Directive 2000.12, "Combating Terrorist Program". As opposed to the "advisory" role that it once had, the DOD Handbook 2000.12H is now "Directive" in nature. It is the new DOD standard.<sup>120</sup>

Through these two cases it is clear that protection from the threat of terrorism is key to the operational chain of command. In each case commanders were held responsible for their lack of attention to the terrorist threat. Although neither of these

cases involved the U.S. Army, the fact that the Army has not been targeted is only chance. The Army's involvement in peacekeeping operations throughout the world provides terrorists with opportunities like Beirut and Saudi Arabia on a daily basis. Just as in these cases, an attack on Army personnel or facilities could have a dramatic strategic impact on U.S. foreign policy.

In order to evaluate the Draft FM 100-5 *Operations*, this monograph will use the failings of the operational chain of command from these two case studies to select portions of the DOD Directive 0-2000.12-H to evaluate the draft FM in its adequacy to protect the Army from the terrorist threat. These areas of focus will be intelligence, lack of understanding the threat, lack of proactivity by commanders, staffing, training, and commander's responsibility.

### **SECTION III - DOD DIRECTIVE 0-2000.12-H**

#### **INTRODUCTION**

In Section II of this monograph six areas of commonality between the Beirut and Dhahran bombings were found which relate directly to the operational commander. In each case study, intelligence was available to warn of the terrorist threat but it went unheeded. As a result, the operational commanders did not understand the threat. This lack of understanding caused a lack of proactivity by commanders and staffing and training became inadequate to face the terrorist threat. While the lack of proactivity by commanders due to their lack of understanding the threat may be attributed to the events

surrounding their situations, both the Long Commission and the Downing Task Force found that the commanders were responsible for protection of their forces.

As a result of the Khobar Towers bombing in Saudi Arabia Secretary of Defense William Perry changed the nature and scope of Department of Defense Directive 0-2000.12. Previously, the DOD Directive had been advisory in nature and was only an aid to antiterrorism planning and training. After the Saudi attack, the Secretary of Defense ordered that it be used as the DOD standard and made it directive in nature. It is now *the DOD standard*.<sup>121</sup>

The DOD Directive 0-2000.12 (hereafter referred to as the *Directive*) itself is only a tool that assigns responsibilities for the protection of DOD personnel and their families, facilities, and other material resources from terrorist acts.<sup>122</sup> The document that drives the actual implementation of the policy is DOD Directive 0-2000.12-H. DOD Directive 0-2000.12-H (hereafter referred to as the *Handbook*) is the DOD Handbook that actually sets forth guidelines.

#### **DOD DIRECTIVE 0-2000.12-H**

The DOD Combating Terrorism Program has two phases. The first phase is the preventive phase in which all DOD elements identify the threat; assess the risk, vulnerability and criticality of installations, personnel, and material; promote awareness and conduct training of personnel in preventive measures; and develop plans to prevent, respond to , contain and resolve terrorist incidents should they occur. The second phase, which is the reactive phase, involves the implementation of crisis management plans and resolution of the terrorist incident. While the *Handbook* encompasses actions to be taken

from the National Command Level to the individual soldier, this monograph will focus primarily on the operational level.

This section will use the portions of the *Handbook* which focus on the commonalties found between the two cases studies to extract the appropriate guidance from the *Handbook* which would correct the mistakes found common in both case studies. To do this, the section will be divided into three sub-sections. The first will be Intelligence, which will focus on terrorist groups and their methods, availability of terrorist threat intelligence, and the DOD Threat Analysis Systems. The second will be Understanding the Threat, which will explain the Integrated Terrorist Threat Estimate. The third will be Training, which will explain unique individual and staff training to thwart the terrorist threat.

## **INTELLIGENCE**

In both case studies, intelligence sources were found to have had information that should have provided adequate warning to the forces that were attacked. Unfortunately, the warnings were either not interpreted or not understood. This misunderstanding of the terrorist threat is a key linkage to overall force protection. The intelligence portion of this section will examine what the *Handbook* says with regards to threat identification and threat analysis.

### **Threat Identification**

In order to successfully combat the terrorist threat, the operational commander must have an understanding of the organization, tactics, and goals of the terrorist group that he faces. The initial step in the development of a combating terrorism program is an

analysis of the threat of terrorism.<sup>123</sup> The *Handbook* details all aspects of the terrorist threat. The main ideas are summarized here to form a baseline from which to identify and understand the terrorist threat.

### **Terrorist Group Organization**

In order for a terrorist group to succeed, it must have effective leadership and dedicated followers within the group. Additionally, it must have dedicated followers outside of the group to provide above ground support such as intelligence collection and fund raising.

Internal personnel of the terrorist group include the hard-core leadership and the active cadre. At the top level of the terrorist group is the hard-core leadership. These persons are typically educated, charismatic and upper-class. If the group is state supported or state-directed the leadership will normally include one or more persons with extensive training from the sponsoring state.<sup>124</sup> At the second tier of command is the active cadre, which are the soldiers of the group. These personnel conduct attacks, assassinations and bombings as well as intelligence collection. At this level the deranged, sociopaths or psychopaths are found.<sup>125</sup> These are the “true believers”.<sup>126</sup>

External to the actual terrorist group are the active and passive supporters. Beneath the active cadre are the active supporters. These people are not actually members of the group but provide support and will go to various extremes to support the groups actions. These people interact with the leadership and cadre and are aware of the true nature of the group. They may collect intelligence and provide logistical support. They may even play minor, safe roles in terrorist operations.<sup>127</sup> The second level of

supporters are known as the passive supporters who acknowledge the presence of terrorists in their homes, neighborhood, or business but chose to ignore such activities.<sup>128</sup>

### **Types Of Terrorist Attacks**

Terrorists have many techniques at their disposal to accomplish their goals. The most common ones likely faced by the operational level commander are presented here for comparison.

Assassination, which is only a euphemism for murder, is generally applied to the killing of a prominent person or symbolic enemy.<sup>129</sup> The goal may not be to dispose of the individual target as much as it is to show weakness and vulnerability of the victims' institution. Assassination is also widely used against traitors who defect from the group to deliver a message of expected loyalty to current members.

Bombing is another terrorist tactic that is their most popular tool. Improvised Explosive Devices (IED) can be very cheap to produce, and because of advanced detonation technology are of low risk to the perpetrator. Bombs have a great attention-getting capability and casualty control is made easy through placement and time of detonation. Bombs are easily denied if the expected result is not obtained. From 1983 to 1990, one half of terrorist incidents involved bombs.<sup>130</sup>

Hostage taking, the overt seizure of people to gain publicity or concessions in return for release of the hostage(s), is a very dramatic terrorist technique. This technique, however, provides one of the highest risks to the terrorist when used in an unfriendly environment.<sup>131</sup>

Kidnapping, unlike hostage taking, is the covert seizure of person(s) in order to extract specific demands. Identity of the perpetrators is easily concealed for a long time and media coverage will be initially intense, but will fade over time. Kidnapping requires detailed planning and logistical support for the terrorist but the risk is less than for hostage taking.<sup>132</sup>

### **Types of Terrorist Groups**

The tactics and target selection of a terrorist group is normally a function of that group's affiliation, training level, organization and sophistication. Accordingly, security forces categorize terrorist groups according to their operational traditions: national, transnational, or international. National groups operate within the boundaries of a single nation. Transnational groups operate across international borders. International groups operate in two or more nations and are usually assumed to receive direction and support from a foreign government.<sup>133</sup>

Another categorization of terrorist groups is determined by their level of government affiliation. The first of these categories is the non-state-supported group, which operates independent of government direction and receives little, if any support. The second group is the state-supported group, which operates independent of government control, but receives state support from one or more governments. The third group is the state-directed group. These terrorists operate as an agent of the government and receive substantial support in the form of intelligence, logistics and funding.<sup>134</sup> These categories are useful to planners to help them anticipate target selection and determine the level of threat.

## **Threat Analysis Organizations (CINC)**

There are a number of national assets available to assist the operational commander in combating terrorism. The Central Intelligence Agency(CIA), Department of Justice(DOJ), Federal Bureau of Investigation(FBI), Department of Energy(DOE), Department of State(DOS), Department of Transportation(DOT), and DOD all are extensively involved in combating terrorism. The operational commander has access to most of this assistance is through his geographical CINC.

The operational commander can expect a great deal of assistance from his geographical CINC. The *Handbook* prescribes many responsibilities that a Geographical CINC must perform. First, he must establish command policies and programs for the protection of DOD personnel, facilities and material resources from terrorist attacks. Second, he must assess the terrorist threat for the theater and provide a copy of the threat assessment to the Military Services. Third, he must keep subordinate commanders informed of the nature and degree of the local threat and ensure that commanders are prepared to respond to threat changes. Fourth, he must assist subordinate commanders in implementing their antiterrorism programs. Last, he must serve as the DOD point of contact with U.S. embassies and host-nation officials on matters involving antiterrorism policies and measures.<sup>135</sup>

Although the CINC has the preponderance of the responsibility for antiterrorism protection and policies outlined in the *Handbook*, the operational commander must insure that his concerns and situation assessments reach the CINC level to insure that his specific needs are met by assets at the CINC's disposal. It is his responsibility to insure



that all appropriate measures are taken to protect his soldiers. He must insure a knowledge of the organization, tactics, type of terrorist groups and know where to access the information in order to conduct a thorough analysis. The assets are available, he must insure that he asks the right questions and conducts a thorough assessment of his particular situation.

### **Threat Analysis**

Threat analysis is the key to threat assessment and the first step in combating terrorism. The primary intelligence mission in support of DOD combating terrorism program is warning.<sup>136</sup> To conduct this analysis there are many sources. Some to them are open source material, criminal investigations, government information, local information and the intelligence system.<sup>137</sup> Many times the operational commander is in the best place to collect the most critical link in a terrorist operation: local information. The information that he collects locally will not only help to protect his own forces, it can be fed to the CINC level assets and help paint a better picture for the entire region when integrated with existing intelligence.

In order to plan a Combating Terrorism Program, the operational commander must understand the DOD Terrorist Threat Condition System. As part of the DOD's comprehensive approach to combating terrorism, a common framework of protective measures against terrorist threats has been developed for implementation by all DOD components. The two parts of the system are the Terrorist Threat Level and the Terrorist Threat Condition.<sup>138</sup>

The first system is the Terrorist Threat Level System. They are one word descriptors which summarize the DOD-level intelligence analysis of the threat of terrorism to DOD personnel, facilities, material and assets on a country by country basis.<sup>139</sup> There are five Terrorist Threat Levels: Critical, High, Medium, Low and Negligible. The specific level is based on a compilation of the factors of Existence, Capability, History, Intentions, Targeting and Security Environment by a terrorist group in a particular area.<sup>140</sup>

The six threat level analysis factors which are used to assess terrorist threat levels are the existence of the a terrorist threat in the area, the capability of existing terrorist groups to conduct an attack, intentions of a group to oppose U.S. presence or actions, the demonstrated terrorist activity over a period of time, targeting information on activity in the local area, and the assessment of the local security and political environment.<sup>141</sup> The operational commander can be key to developing information on the targeting and security environment aspects of this evaluation. Table 1 shows the interrelationship of these factors.

<b>Table 1: Threat Analysis Factors and Terrorist Threat Levels</b>					
Threat Level	Existence	Capability	History	Intentions	Targeting
Critical	o	o	x	x	o
High	o	o	o	o	
Medium	o	o	o	x	
Low	o	o	x		
Negligible	x	x			
o = factor must be present      x = Factor may or may not be present * The factor, Security Environment, which assesses the ability of police, paramilitary and military institutions to preserve local order, may be a mitigating factor. Countries which have effective internal security institutions may be assessed at a lower threat level on that basis.					

Once these criteria have been evaluated, the DOD uses a five step scale to describe the severity of the threat as judged by intelligence analyst. The five categories are, in descending order, critical, high, medium, low, and negligible.<sup>142</sup> While these assessments are a valuable tool to the operational commander, they do not tell when and where an attack might occur, they do not allocate protective resources, and they do not act as a warning notice.<sup>143</sup> "It remains the responsibility of the commander in the field ... to allocate protective measures."<sup>144</sup>

The second system is the Terrorist Threat Condition (THREATCON) System. This system describes the progressive level of protective measures implemented by all DOD components in response to terrorist threats in accordance with *Directive*. The declaration of the THREATCON is the prerogative of the military commander. Generally, lower echelons should adopt the THREATCON as that of the CINC, however, local commanders may adopt higher THREATCON measures than ordered by the chain of command if local conditions warrant greater protection. There are five THREATCON levels. The circumstances and purposes are listed below:<sup>145</sup>

- NORMAL - applies when a general threat exists, but only warrants routine security.
- ALPHA - applies when there is a general threat of possible terrorist activity against personnel and installations, the nature and extent of which are unpredictable.
- BRAVO - applies when an increased and more predictable threat of terrorist activity exists.
- CHARLIE - applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel and installations is imminent.
- DELTA - applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location is likely. Normally, THREATCON DELTA is declared as a localized warning.

Commanders and staffs must be aware that the increase in THREATCON costs in terms of time, dollars, and personnel productivity.<sup>146</sup> To reduce these “costs” the commander can use Random Antiterrorism Measures(RAM).<sup>147</sup> The RAM uses selected precautions of the higher THREATCONs in a random fashion. It enables the commander to test antiterrorism measures, to train security forces and to quickly change the security posture of the local area. An additional benefit of the RAM is that it changes the patterns and cause difficulties for terrorist planners. RAMs are not “free” but they are an excellent alternative to increasing THREATCONs.

## **UNDERSTANDING THE THREAT**

Once the evaluation of the Threat Level and THREATCON has been established, the operational commander must take the second step in combating terrorism, which is to evaluate the risk, vulnerability and criticality of his forces. This assessment, integrated with the threat level and THREATCON will provide an understanding of the terrorist threat in his area.

### **Integrated Terrorist Threat Estimate**

The second step in a combating terrorism program is the assessment of risk, vulnerability, and criticality. This is done through the Integrated Terrorist Threat Estimate. This estimate must be done by commanders and staffs at all levels within the DOD components.<sup>148</sup>

### **Risk**

Assessments of the risk of a terrorist attack seeks to understand the circumstances under which an attack is more or less likely and how leaders can reduce the likelihood of

an attack.<sup>149</sup> Much of the information needed to begin a risk assessment will be from the Defense Intelligence Agency(DIA). "Assessing of the risk of becoming the victim of a terrorist attack is the responsibility of ... command at every echelon. It is a responsibility that cannot be delegated or waived".<sup>150</sup> The risk of becoming a victim of terrorist attack can be influenced by several factors.

Understanding the terrorist group's goals and objectives (addressed above) are the first step in the risk assessment.<sup>151</sup> It is important that all levels of command understand the political situation in which the military mission occurs and to use that information to determine if the attack on the unit would help achieve the terrorist groups goals. Even if an attack on the particular unit would not help achieve the terrorists goals and objectives, commanders need to assess whether their proximity to other facilities or personnel (e.g. host-nation military or facilities) could cause them to become inadvertent victims of an attack.<sup>152</sup>

While the *Handbook* extensively explains that the mere fact that someone may become a victim of terrorist attack just for being an American, the assumption to the operational commander is that this will be obvious in a military mission. There are however, two aspects of this which are relevant. The first is detectability. If the terrorist cannot detect his necessary target, he cannot attack it. The second is accessibility. If the terrorist cannot gain access to a specific target, he is likely to look elsewhere for a target to achieve his goals. The commander must take measures to prevent critical assets from being detected or being identified as critical and then restrict a terrorist from accessing those assets.

## **Vulnerability**

The purpose of vulnerability assessments are to understand the compound probability of being hit by a terrorist attack and whether or not the mission can be completed if an attack occurs. The vulnerability assessment seeks to find weakness in physical security plans, inefficiencies of personnel practices and identify resource requirements.<sup>153</sup> The assessment process begins by “thinking like a terrorist” to determine what targets are lucrative for a terrorist attack, determining early warning signs and assessing how well these likely targets are protected.

The physical security assessment is conducted on all visible, fixed land based DOD facilities within the treat area. Included in this assessment is the protection of senior military officers. These personnel must be protected as in some cases, loss of an individual is tantamount to the failure of a DOD mission. The physical security assessment must be an ongoing process.<sup>154</sup>

## **Criticality**

The criticality assessment identifies key assets that support DOD missions, units, and activities and are deemed critical to mission accomplishment. It addresses the impact of temporary or permanent loss of key assets. Additionally, it examines costs of recovery and reconstitution in terms of time, dollars, and capability.<sup>155</sup> In some missions, like Beirut, the single event may be critical enough to cause mission failure.

These assessments are not the sole province of the intelligence community. The operational commander must insure an integrated staff effort to insure that threat assessment is well integrated into the risk assessment to provide a complete picture. In

order to provide this integration the commander must insure that the staff understand the threat and is trained to take measures to prevent a terrorist attack.

## **TRAINING**

While an understanding of the terrorist threat is essential to combating terrorism, training is also critical. There are two important elements to antiterrorism training. The first is the individual training in individual protective measures which will promote general awareness of the threat at the individual level, and the second is staff training which will allow the staff to integrate planning toward total force protection and react to a terrorist incident if it should occur.

### **Promote Awareness and Conduct Individual Training**

Individual protective measures, while primarily the concern of tactical commanders, must not go overlooked by the operational commander. He must insure individual training is conducted to prepare soldiers to survive in an environment with a terrorist threat as poor individual actions can collectively increase the vulnerability of the entire unit. The key elements to this training must address reduction of routines, maintenance of a low profile, and a general awareness of the terrorist threat.<sup>156</sup> As importantly, soldiers must be trained in hostage survival<sup>157</sup> and Code of Conduct<sup>158</sup> as it applies to terrorist situations.

### **Staff Training: Proactive Training**

The *Handbook* provides a section on “Combating Terrorism Practices For Expeditionary And Deployed Forces”. This portion of the *Handbook* is an excellent guide for all forces, especially those at the operational level.

Deployed forces must take combating terrorism measures at the unit and individual level. The purpose of the combating terrorism plan is to provide the mechanism to ensure readiness against terrorist attacks while units perform their assigned mission. Commanders of deployed forces are responsible to continually evaluate the situation. It is his responsibility!

The first step in development of the combating terrorism plan is the estimate of the situation. This estimate can be done by using the METT-T analysis format. Table 2 gives examples of questions to ask while performing the analysis.

<b>Table 2: Estimating the Combating Terrorism Situation for Deployed and Expeditionary Forces (Derived From Figure 18-1; p. 18-2)</b>				
<b>MISSION</b>	<b>ENEMY</b>	<b>TERRAIN</b>	<b>TROOPS</b>	<b>TIME</b>
Who is being tasked?	Who are the potential terrorists?	What are the strengths and weaknesses of the location?	Determine friendly situation.	Determine duration of mission.
What is the task?	What is known about them?	Are avenues of approach above and/or below ground?	Are other U.S. forces or equipment available?	Are there time constraints?
When and where is the task to take place?	How do terrorists obtain information?	Are there observation areas, dead spaces, fields of fire; schools, hospitals, etc.?	Are engineers in the area? Can they provide support?	Will there be time to construct force protection facilities; barriers, fences, lights?
Why are we doing the task?	How might terrorists attack? (Ambush, raid, sniper, air attack, vehicle bomb, suicide attack)	Are there tall buildings, structures, or terrain that could become critical in an attack?	Are emergency reinforcements in the area?	
	Does the unit have routines?		What are the host-nation responsibilities, capabilities, and attitudes toward providing assistance?	
	What is the potential for civil disturbance?			



	Could terrorists use disturbances in an attack?			
	Do you have good contacts w/ local law enforcement, host-nation security who can provide threat information?			

Once the estimate has been completed based on the threat identification and threat analysis, the second step is development of the combating terrorism plan. The plan should include a combination of local law enforcement, fortifications, sensors, obstacles, local-hire security forces, unit guards, deception and on-call reactionary forces.<sup>159</sup>

There are five considerations which the combating terrorism plan must make that may not be part of the norm for a conventional military unit. The first is road movement. Military road movements tend to establish specific routes and times for execution. In an environment with a terrorist threat is imperative that movements avoid regular patterns and must vary routes and times. If the pattern is established, the terrorist will have a distinct advantage in planing an attack. For convoys, the commander should consider armed escort vehicles or armed aerial support.<sup>160</sup> The second consideration is training observation post personnel on the specific patterns to look for that the terrorist group may use to target the unit. Their observations and immediate response can be key in thwarting a terrorist attack.<sup>161</sup> The third consideration is the response to civil disturbances. This crowd violence may be a precursor to a terrorist attack by drawing military forces to one area to attack it, or by using the violence to draw military forces away from the area to be attacked. The fourth consideration is the response to a bomb explosion or discovery. The

initial terrorist bomb may not be the end of the incident, but be designed to draw forces into an area as targets for a shooting ambush or another explosion.<sup>162</sup> The last consideration is rear area protection. These areas are typically lucrative and relatively unprotected targets. They must given adequate protection commensurate with the terrorist threat.<sup>163</sup>

Unlike “stationary” forces, these tasks will normally be conducted in an already hostile or unfamiliar environment. The main elements to force protection for deployed forces is to avoid routines, maintain a low profile, and be sensitive to changes in the security atmosphere and environment.

#### **Staff Training: Reactive Training**

Notwithstanding efforts to prevent a terrorist incident, commanders at all levels must be prepared to respond to a terrorist incident. While the terrorist incident in itself can be disastrous, poor handling of the event can make the situation even worse.

At the onset of an incident, four questions must be answered by the responding force. The first information required is the type of asset in danger, from non-essential to mission essential property. Second, the type of harm or danger to DOD assets. This is to determine whether it is only property or if personnel are involved. The third question that must be answered is the imminence of jeopardy of danger to DOD assets. This determines the immediacy of the problem. The last question to be answered is the scope, magnitude and intensity of jeopardy to additional DOD assets and civilians. This seeks to identify the area affected by the terrorist event.<sup>164</sup>

Next, the initial response force must identify, report and isolate the incident and seek medical attention as required. The local commander must activate the Emergency Operations Center or Tactical Operations Center to control the events surrounding the incident. Lastly the commander must confirm jurisdiction for the event and request necessary additional forces.

There are several special considerations that may be unique for a terrorist attack. They are 1) insuring available communication is available to control the responding forces; 2) insuring evidence is protected for further investigations; 3) apprehension of suspected personnel; 4) insuring accurate and immediate reporting of the incident; and 5) insuring that the Public Affairs is properly coordinated.<sup>165</sup> The key to handling a terrorist attack is planning, preparation and training.<sup>166</sup>

One aspect of the reaction to a terrorist incident that must be planned is public affairs. All DOD commands should have an ongoing public affairs program intended to reduce its risk and vulnerability to a terrorist attack. There are four objectives for the Combating Terrorism Public Affairs Plan. The first is to increase awareness of the terrorist threat, the second is to maintain good communications with surrounding communities, the third is to provide timely, accurate, and authoritative information on terrorist attacks to counter rumors, and the forth is to provide authoritative information to news media on incidents.<sup>167</sup>

### **SECTION III CONCLUSIONS**

The *Handbook* provides guidance that can correct the deficiencies found in both the Beirut and Dhahran case studies through a thorough understanding of the terrorist

threat picture coupled with risk assessment and proper individual and staff training. Its contents can focus the intelligence to provide a common understanding to the command and staff so that they can provide resources and training to adequately protect their forces.

The findings of this section will serve as a guideline to evaluate the Draft FM 100-5 *Operations* as to how it addresses the terrorist threat for the operational commander. Section IV will use the guidance provided by the *Handbook* in the areas of intelligence, threat understanding and training to conduct the assessment.

## **SECTION IV - TERRORISM AND DRAFT FM 100-5**

### **INTRODUCTION**

U.S. Army FM 100-5 *Operations* is the Army's keystone warfighting manual. Its goal is to address the full range of operations that the Army expects to execute in the foreseeable future -- offensive, defensive, stability and support operations.<sup>168</sup>

While the 1998 FM 100-5 *Operations* is not intended to be a manual that focuses solely on the terrorist threat, it must heighten the commanders attention to that threat to insure adequate force protection for the Army of the future. Because of the nature of the manual and its ability to focus the attention of the operational commanders and staffs and to shape the doctrine that is written in the future, it must address the terrorist threat in sufficient detail to insure that those faced with the threat will be aware of its significance to the Army.

This section of the monograph will review the Draft FM 100-5 *Operations* to determine what it currently says regarding the terrorist threat to determine whether it

addresses the three major topics extracted from the DOD 0-2000.12 Handbook in Section III of this monograph; Intelligence, Understanding the Threat and Training.

## **FM 100-5 OPERATIONS: WHAT IT SAYS**

*Operations* addresses the terrorist threat in Part IV, Chapter 3: Stability Operations. The entire text from the two places where it is addressed, Stress Force Protection and Combating Terrorism, will be presented here to provide a point of departure for evaluation:

### **Stress Force Protection**

Commanders must take great pains to protect the force from attack. Adversaries seeking to destabilize an area will of to great length to expel US forces to advance their agendas. Actions they will employ include terrorist type bombings, minings, kidnappings, assassinations, ambushes, and raids.

Adversaries threaten the force to threaten the mission. Their aim is to cause a collapse of American will. Attacks on American forces conducting stability operations tend to fall into two broad categories: sensational terrorism and force-on-force. Commanders must always be prepared to counter the first (See Anti-terrorism operations). Depending on circumstances, they must also be prepared to counter the second.<sup>169</sup>

### **Combating Terrorism**

Enemies who cannot compete with Army forces at the conventional level often turn to a different arena -- terrorism. Terrorism is a historically proven means of attacking *and defeating* the most capable of conventional forces. Terrorist attack using a wide array of tactics, including:

--Arson	--Assassination	--Bombing
--Hijacking	--Hostage-taking	--Kidnapping
--Maiming	--Sabotage	--Raids
--Seizure	--Hoaxes	--Use of NBC for hysteria

Army forces conduct combating terrorism operations to defeat attacks. These operations contain both offensive and defensive components. Offensive operations are counterterrorism; defensive

operations are antiterrorism. The Army participates in counterterrorism operations outside the territory of the United States, while it conducts antiterrorism anywhere in the world.

### ***Counter Terrorism***

Army forces participate in the full array of counterterrorism actions, including strikes and raids. Against organizations and facilities. Normally this involves special operations forces operating under a unified command arrangement. However, it may involve a commander employing conventional forces to strike against organized terrorist forces operating inside his area of operations in a combat zone.

### ***Anti Terrorism***

Antiterrorism includes all defensive measures taken to reduce the vulnerability of personnel, installations, facilities, and equipment to attack. antiterrorism must be a priority of all forces on *all* operations--offensive, defensive, stability, and support. Experience shows that sensational acts of terrorism against US forces can have strategic impacts. We must take great pains to protect the mission by protecting the force against terrorism.

Typical Anti-terrorism actions include:

- Coordination with local law enforcement
- Siting and hardening of facilities
- Physical security actions designed to prevent unauthorized access or approach to facilities
- Crime Prevention/Physical security actions that prevent theft of weapons, munitions, Identification cards, and other materials.
- Policies regarding travel, size of convoys, breaking routines, host-nation interaction, and 'off-duty' restrictions.

Army forces are often most vulnerable in "off-duty" periods and locations. Soldiers and families that reside outside protected installations make ideal targets to terrorist and other hostile agents. Commanders must take every effort to minimize the potential for of murders and hostage takings being used as a means to thwart stability efforts.<sup>170</sup>

## **SECTION IV CONCLUSION**

The Stress Force Protection and Combating Terrorism sections clearly indicate that the authors of the new *Operations* understood the methodology, importance and seriousness of the terrorist threat. Section V of the monograph will evaluate whether the

authors included the aspects of the terrorist threat distilled from the DOD Handbook in Section III to the extent required by the operational commander.

## **SECTION V - RECOMMENDATIONS AND CONCLUSIONS**

### **INTRODUCTION**

Section V will evaluate the terrorism portion of the new *Operations* in accordance with the criteria established in Section III in the areas of Intelligence, Understanding the Threat and Training. It will then answer the research question and make recommendations.

#### **Intelligence**

Sections II and III of this monograph demonstrated that a commander cannot defeat the terrorist threat without a detailed understanding of that threat. While *Operations* gives examples of the types of tactics that a terrorist group may use to achieve their goal, it does not address the types of terrorist groups or terrorist group organization. For this type of manual it is not necessary to extensively explain the different types, but it would very helpful to give the reader a list of examples and give a reference to where further information can be located in other manuals.

*Operations* also does not give the locations where commanders and staffs can get information on the terrorist threat, or give examples of how to analyze the threat that they may face. Further, it does not address Threat Analysis or RAM. Again, *Operations* does not need to give a detailed explanation of these concepts, but it would be very helpful to give the reader a reference for additional information.

## **Understanding the Threat**

Sections II and III showed the importance of understanding the terrorist threat. Without this understanding the commander and staff cannot properly focus his efforts to combat terrorism. *Operations* makes no mention of the Integrated Terrorist Threat Estimate, which can assist the commander and staff determine their Risk, Vulnerability and Criticality as a target. Once again, *Operations* need not give a detailed explanation of the concept, but to mention it and give a reference should be very useful to readers because it would make them aware of tools that are available.

## **Training**

In the Anti Terrorism section of *Operations* there is a short list of actions that can be utilized to defend against terrorism. Further, this part of the manual acknowledges that the individual soldier is vulnerable in activities not necessarily related to his military performance. While this is probably enough for this type of manual, it does not point out that to conduct these preventive measures will require training above and beyond what may normally take place for a conventional force. *Operations* does not give a reference to a publication which would provide further guidance on the subject of specific individual and staff training for the terrorist threat.

## **RECOMMENDATIONS**

With a few additions the section on Combating Terrorism in the new *Operations* could be made adequate. The main problem with subject of terrorism in the new *Operations* is that it only addresses the terrorist threat in the section on Stability Operations. This would lead the reader to believe that the only time he would face a



terrorist threat was under those circumstances. While this is a likely occurrence, the terrorist threat is constant throughout the spectrum of conflict.

In Chapter 1, *Operations* uses the concept of Asymmetric Advantage.<sup>171</sup> One of the aspects of this advantage is dissimilarity, which “forces an opponent to fight against things for which he has no design or capability”.<sup>172</sup> This concept is to attack the weak point of the enemy. It is the concept which *Operations* will lead toward for the Army of the future. It is also the advantage that the terrorist has over a conventional military force. Section II of this monograph showed two instances where the terrorist threat was overlooked and underrated because the terrorist had the Asymmetric Advantage. In order to prevent an act of terrorism from affecting the Army as it has the Marine Corps and Air Force the Army must insure that it has a capstone doctrine which will adequately focus the operational commander on the terrorist threat and reduce the Asymmetric Advantage.

## CONCLUSIONS

The principle research question for this monograph is: “Does The 1998 FM 100-5 Adequately Address Terrorism at the Operational Level of War for the Army of the 21st Century?” The answer is no. The Draft FM 100-5 *Operations* concedes that the enemies that cannot compete with U.S. Army forces will turn to terrorism<sup>173</sup> and that “antiterrorism must be a priority for all forces on *all* operations--offensive, defensive, stability, and support. Experience shows that sensational acts of terrorism against US forces can have strategic impacts.”<sup>174</sup> Terrorism is a threat in all levels of war and in all missions. The key to protection against the terrorist threat is the ATTITUDE of the leadership<sup>175</sup> and AWARENESS of the threat.<sup>176</sup> In order to properly inculcate Force

Protection against the terrorist threat into the core of Army operations and missions, *Operations* must address the threat throughout the manual, not simply in one section. The Appendix to this monograph will make specific recommendations as to where and how the manual can thoroughly include Force Protection against the terrorist threat for the operational commander.

## ENDNOTES

<sup>1</sup> U.S. Army, Field Manual 100-5 *Operations* (Coordinating Draft), (Ft. Leavenworth, KS; Combined Arms Center, 14 January 1997, I-1-5.

<sup>2</sup> Ibid., ii.

<sup>3</sup> Ibid., i.

<sup>4</sup> Joint Chiefs of Staff, Joint Pub 3-0 *Doctrine for Joint Operations*, (Washington, DC: Department of Defense, 1 February 1995), II-1.

<sup>5</sup> Ibid., II-2.

<sup>6</sup> Ibid., II-1.

<sup>7</sup> Ibid., II-2.

<sup>8</sup> Ibid., II-2.

<sup>9</sup> Ibid., II-2.

<sup>10</sup> Ibid., II-2.

<sup>11</sup> Ibid., II-3.

<sup>12</sup> Ibid., II-3.

<sup>13</sup> Ibid., p II-3.

<sup>14</sup> Ibid., p II-2.

<sup>15</sup> Ibid., II-2.

<sup>16</sup> Ibid., II-3.

<sup>17</sup> Carl Von Clausewitz, *On War*, trans. Michael Howard and Peter Paret. (Princeton: Princeton University Press, 1976), 89.

<sup>18</sup> Ibid.

<sup>19</sup> Ibid.

<sup>20</sup> United States Government, "Report of the DOD Commission on Beirut International Airport Terrorist Act, October 23, 1983", 20 December 1983, 54-55.

<sup>21</sup> United States Government, "Force Protection Assessment of USCENTCOM AOR and Khobar Towers, Report of the Downing Assessment Task Force", 30 August 1996, xviii.

<sup>22</sup> Joint Chiefs of Staff, Joint Pub 1-02 *Department of Defense Dictionary of Military and Associated Terms*, (Washington, DC: The Joint Chiefs of Staff, 1994), 151.

<sup>23</sup> Ibid., 399.

<sup>24</sup> Department of Defense, Joint Pub 3-07.2. *Joint Tactics, Techniques, and Procedures for Antiterrorism*, (Washington, DC: Department of Defense, 1993), I-1.

<sup>25</sup> G. Wardlaw, *Political Terrorism*, (NY: Cambridge Univ. Press, 1989), 16.

<sup>26</sup> Joint Pub 1-02, 97.

<sup>27</sup> Joint Pub 3-07.2, I-1.

<sup>28</sup> Joint Pub 1-02, 30.

<sup>29</sup> Ibid.

<sup>30</sup> U.S. Marine Corps, FMFM 7-14 *Combating Terrorism*, (Washington, DC: Department of the Navy, 1990), 1-4.

<sup>31</sup> R. McLaurin and R. Miller, *Military Forces in Urban Antiterrorism*, (Springfield, Va.: Abbott Associates Inc., 1989), 11.

<sup>32</sup> Ibid., 11-15.

<sup>33</sup> Joint Pub 3-07.2, II-8.

<sup>34</sup> E. Evans, *Calling a Truce to Terror*, (Westport, Conn.: Greenwood Press, 1979), 26.

<sup>35</sup> Ibid., 29.

<sup>36</sup> Ibid., 31.

<sup>37</sup> Ibid., 32.

<sup>38</sup> Ibid., 33.

<sup>39</sup> "Beirut Terrorist Act", 24.

<sup>40</sup> Ibid., 28.

<sup>41</sup> Ibid., 8.

<sup>42</sup> "Beirut Terrorist Act", 29; McLauren, 94.

<sup>43</sup> "Beirut Terrorist Act", 29.

<sup>44</sup> Ibid., 14.

<sup>45</sup> E. Hammel, *The Root: The Marines in Beirut, August 1982 - February 1984*, (NY: Harcourt Brace Jovanovich, Publishers, 1985), 38-39.

<sup>46</sup> "Beirut Terrorist Act", 2-4.

<sup>47</sup> Ibid., 39.

<sup>48</sup> Ibid., 3.

<sup>49</sup> Hammel, 42.

<sup>50</sup> "Beirut Terrorist Act", 40.

<sup>51</sup> Ibid., 41.

<sup>52</sup> Hammel, 112.

<sup>53</sup> "Beirut Terrorist Act", 40.

<sup>54</sup> Ibid., 32.

<sup>55</sup> Ibid., p. 6.

<sup>56</sup> Ibid., 94.

<sup>57</sup> Ibid., 3; 32-33.

<sup>58</sup> Ibid., 33.

<sup>59</sup> United States Marine Corps. FMFRP 7-14A *Individual's Guide for Understanding and Surviving Terrorism*, (Washington, DC: Department of the Navy, 1989), 1-1.

<sup>60</sup> McLauren, 126.

<sup>61</sup> Ibid., 109.

<sup>62</sup> McLaurin, p. 109.; The "Beirut Terrorist Act" Report states that the environment was clearly hostile to the USMNF by the end of September 1983, 40.

<sup>63</sup> Hammel, 423.

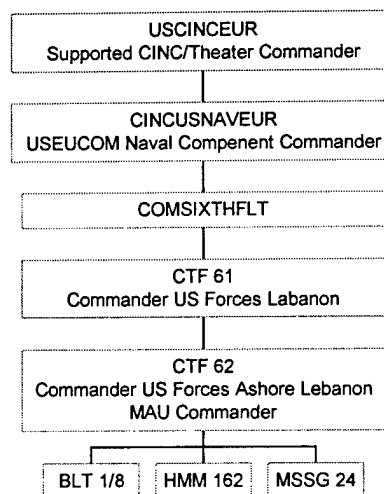
<sup>64</sup> D. Vought, "The Coming Age of Terror" in *Security Intelligence Sourcebook*. ed. F. McGuire, (Silver Spring, Md.: Interests, Ltd, 1993), 15.

<sup>65</sup> "Beirut Terrorist Act", 15.

<sup>66</sup> Ibid., 3.

<sup>67</sup> Ibid., 7; 10.

<sup>68</sup> Ibid., 52. The operational chain of command at the time of the USMNF bombing:



<sup>69</sup> "Beirut Terrorist Act", 54.

<sup>70</sup> Ibid., 54.

<sup>71</sup> Ibid.

<sup>72</sup> Ibid., 53.

<sup>73</sup> Ibid.

<sup>74</sup> Ibid., 6.

<sup>75</sup> Ibid., 56.

<sup>76</sup> McLauren, 17.

<sup>77</sup> Ibid., 99.

<sup>78</sup> Secretary of Defense, Report to the President "Force Protection: Global Interest, Global Responsibilities". 16 September 1996, 2.

<sup>79</sup> Ibid., 2.

<sup>80</sup> Ibid., 4.

<sup>81</sup> "Downing Report", 29.

<sup>82</sup> Secretary of Defense, 1.

<sup>83</sup> "Bombs in the Desert", *U. S. News & World Report*, 07 August 1996. ; Secretary of Defense Report to the President, 5.

<sup>84</sup> Secretary of Defense, 5.

<sup>85</sup> "Downing Report", 29.

<sup>86</sup> Secretary of Defense, "Prepared Statement of William J. Perry, Secretary of Defense, before the Senate Armed Services Committee in Connection with The Saudi Arabia Bombing", 9 July 1996, 2.

<sup>87</sup> "Downing Report", 29.

<sup>88</sup> Ibid.

<sup>89</sup> "Telling Friend From Foe", *U.S. News & World Report*, 27 November 1995.

<sup>90</sup> "Bombs in the Desert", 5.

<sup>91</sup> "Downing Report", 17.

<sup>92</sup> Secretary of Defense, 1.

<sup>93</sup> Ibid., 2.

<sup>94</sup> "Downing Report", 21.

<sup>95</sup> Secretary of Defense, 1.

<sup>96</sup> Evans, 26.

<sup>97</sup> "Pentagon Negligence", *New York Times*, 18 September 1996, A 20.

<sup>98</sup> B. Graham, "Perry Accepts Blame In Dhahran Bombing", *Washington Post*, 19 September 1996, A-2.

<sup>99</sup> Evans, 32.

<sup>100</sup> P. Shenon, "United States and Saudis Agree to Split Cost of Safeguarding G.I.'s", *New York Times*, 1 August 1996, 1.

<sup>101</sup> Evans, 31.

<sup>102</sup> *Ibid.*, 32.

<sup>103</sup> F. Kitson, *Low Intensity Operations: Subversion, Insurgency, Peace-Keeping*, (Hamden, Conn.: Archon Books, 1974), 57.

<sup>104</sup> "Downing Report", 15.

<sup>105</sup> "Downing Report", 18.

<sup>106</sup> *Ibid.*

<sup>107</sup> *Ibid.*, 19.

<sup>108</sup> *Ibid.*, 27.

<sup>109</sup> *Ibid.*, 28.

<sup>110</sup> *Ibid.*, 29.

<sup>111</sup> *Ibid.*, 30.

<sup>112</sup> *Ibid.*, 43.

<sup>113</sup> *Ibid.*, 44.



<sup>114</sup> Ibid., 46.

<sup>115</sup> Ibid.

<sup>116</sup> Ibid., 48.

<sup>117</sup> Ibid., 50.

<sup>118</sup> Ibid., 54.

<sup>119</sup> Ibid., 55.

<sup>120</sup> Secretary of Defense, 10.

<sup>121</sup> Ibid.

<sup>122</sup> Department of Defense, Directive 0-2000.12 *DOD Combating Terrorism Program*, (Washington, DC: Department of Defense, 15 September 1996), 1.

<sup>123</sup> Department of Defense, Directive 0-2000.12-H *Protection of DOD Personnel and Activities Against Acts of Terrorism and Political Turbulence*, (Washington, DC: Department of Defense, February 1993), 6-1.

<sup>124</sup> Ibid., 2-4.

<sup>125</sup> Ibid.

<sup>126</sup> For an in-depth review of the concept of the True Believers see E. Hoffer, *The True Believer*, (NY: Harper and Row Publishers, 1951)

<sup>127</sup> DODD 0-2000.12-H, 2-4.

<sup>128</sup> Ibid.

<sup>129</sup> Ibid., 2-8.

<sup>130</sup> Ibid.

<sup>131</sup> Ibid.

<sup>132</sup> Ibid.

<sup>133</sup> Ibid., 2-11.

<sup>134</sup> Ibid., 2-11 - 2-12.

<sup>135</sup> Ibid., 3-8.

<sup>136</sup> Ibid., 5-4.

<sup>137</sup> Ibid., 5-4 - 5-6.

<sup>138</sup> Ibid., 17-1. The Defense Readiness Conditions (DEFCONs) can be confused with these two systems. Although somewhat interrelated, these concepts serve very different purposes and their specific use has vastly different ramifications for the DOD components.

<sup>139</sup> Ibid.

<sup>140</sup> Ibid., 17-2.

<sup>141</sup> Ibid., 5-4 - 5-9.

<sup>142</sup> Ibid., 5-11.

<sup>143</sup> Ibid.

<sup>144</sup> Ibid., 5-15.

<sup>145</sup> Ibid., 17-2 - 17-3.

<sup>146</sup> Ibid., 17-9. Relative expected ability to maintain THREATCONs:

- THREATCON ALPHA: must be capable of maintaining indefinitely.
- THREATCON BRAVO: must be capable of maintaining for weeks w/out causing undue hardship, affecting operational capability, or aggravating host-nation relations.
- THREATCON CHARLIE: implementation of these measure for more than short periods of time will create hardship and affect the peacetime activities for the unit and personnel.
- THREATCON DELTA: Local measure used only for short periods.

<sup>147</sup> Ibid., 17-10.

<sup>148</sup> Ibid., 6-1.

<sup>149</sup> Ibid.

<sup>150</sup> Ibid., 6-2.

<sup>151</sup> Ibid.

<sup>152</sup> Ibid.

<sup>153</sup> Ibid., 6-9 - 6-10.

<sup>154</sup> Ibid., 6-11.

<sup>155</sup> Ibid., 6-13.

<sup>156</sup> Ibid., 12-28.

<sup>157</sup> Ibid., 14-1.

<sup>158</sup> Ibid., 14-11.

<sup>159</sup> Ibid., 18-2.

<sup>160</sup> Ibid., 18-5 - 18-6.

<sup>161</sup> Ibid., 18-9.

<sup>162</sup> Ibid., 18-10.

<sup>163</sup> Ibid.

<sup>164</sup> Ibid., 15-5.

<sup>165</sup> Ibid., 15-9.

<sup>166</sup> Ibid., 15-13.

<sup>167</sup> Ibid., 19-1.

<sup>168</sup> *Operations* (Coordinating Draft), i.

<sup>169</sup> Ibid., IV-3-3.

<sup>170</sup> Ibid., IV-3-15 - IV-3-16.

<sup>171</sup> Ibid., II-1-5 - II-1-6.

<sup>172</sup> Ibid., II-1-5.

<sup>173</sup> Ibid., IV-3-15.

<sup>174</sup> Ibid., IV-3-16.

<sup>175</sup> DODD 0-2000.12-H, 12-4.

<sup>176</sup> Ibid., 12-28.

## APPENDIX - RECOMMENDED CHANGES FOR THE 1998 FM 100-5 OPERATIONS.

- Deletions will be indicated by ~~striketrough~~ text.
- Additions will be indicated by ***bold cased, italicized and underlined*** text.

### **Change # 1 : "Seeing the Enemy" section on p. II-4-4:**

#### Seeing the Enemy

Fourth Paragraph:

"Seeing the enemy, ***whether a conventional threat or a terrorist threat***, is a never ending task that, when done well, pays enormous dividends. When done poorly, it leads to failure."

### **Change # 2 : "Shaping Friendlies" section on p. II-4-9:**

Second Paragraph:

"Commanders shape friendly forces by building units, providing them with the depth of resources required for mission success. Shaping includes the full array of actions inherent in preparing soldiers and units for action, and restoring them to desired capability after action. Rest, reorganization, ~~and regeneration~~ ***and force protection*** are essential to shaping units for sustained operations."

### **Change # 3 : "SHIELD" section on p. II-4-10:**

First Paragraph:

"Constantly, actively shield the force and the operation. Prevent the enemy from acquiring critical information, striking effectively, or moving to counter friendly actions. Shielding includes the full array of active and passive measures used to protect the force and preserve operational security and freedom. It includes actions taken to protect against strikes from all dimensions -- air, ground, maritime, electro-magnetic, ***terrorist***, and psychological."

### **Change # 4 : "Mobility and Survivability" section on p. II-5-9:**

Second Paragraph:

"Engineers operate as an integral member of the combined arms team to provide a full range of mobility and survivability options. In the offense, they concentrate efforts on mobility. In the defense, they concentrate on countering enemy mobility and protecting friendly positions ***from both conventional and terrorist threats***."

**Change # 5 : "THE SITUATION" section on p. III-2-2:**

Paragraph One, Sub-Bullet 2:

- "Planners must consider the dispositions, equipment, doctrine, capabilities and probable intentions of an *enemy* -- actual and potential. The conflict environment today, moreover, is increasingly characterized by shades of gray in which enemies are less apparent. Commanders also evaluate potential *threats* to mission success, such as *terrorism*, disease, political instability, or misinformation."

**Change # 6 : "Linkage" section on p. III-2-13:**

**Linkage**

"Commanders think in terms of battlespace because they know that linkage pervades all aspects of military operations. ... It is in the moral domain, where we shape the will of an adversary, that military operations are ultimately won or lost. *One threat which spans all three domains is the terrorist threat.*"

**Change # 7 : "Stress Force Protection" section on p. IV-3-3:**

**Stress Force Protection**

"Commanders must take great pains to protect the force from attack. Adversaries seeking to destabilize an area will of to great length to expel US forces to advance their agendas. Actions they will employ include terrorist type bombings, minings, kidnappings, assassinations, ambushes, and raids.

Adversaries threaten the force to threaten the mission. Their aim is to cause a collapse of American will. Attacks on American forces conducting stability *ALL* operations tend to fall into two broad categories: sensational terrorism and force-on-force. Commanders must always be prepared to counter the first (See Anti-terrorism operations). Depending on circumstances, they must also be prepared to counter the second."

**Change # 8 : "Reconnaissance and Security Operations" section on p. IV-3-10:**

Paragraph Three:

"Security accounts for the full array of force protection actions. These include procedures for protecting the force and guarding supplies and equipment *from both conventional and terrorist threats*, and interacting with the local populace."

Change # 9 : "Combating Terrorism" section on pp. IV-3-15 - IV-3-16:

## **Combating Terrorism**

"Enemies who cannot compete with Army forces at the conventional level often turn to a different arena -- terrorism. Terrorists use the asymmetry of dissimilarity, just as we do, in an attempt to afford no effective counter to their operations and in doing so, terrorism is a historically proven means of attacking and defeating the most capable of conventional forces. Terrorist attack using a wide array of tactics, including:

- |             |                  |                           |
|-------------|------------------|---------------------------|
| --Arson     | --Assassination  | --Bombing                 |
| --Hijacking | --Hostage-taking | --Kidnapping              |
| --Maiming   | --Sabotage       | --Raids                   |
| --Seizure   | --Hoaxes         | --Use of NBC for hysteria |

The tactics and target selection of a terrorist group is normally a function of that group's affiliation, training level, organization and sophistication. Accordingly, security forces categorize terrorist groups according to their operational traditions: national, transnational, or international. These categories are useful to planners to help them anticipate target selection and determine the level of threat.

- National groups operate within the boundaries of a single nation.
- Transnational groups operate across international borders.
- International groups operate in two or more nations and are usually assumed to receive direction and support from a foreign government.

Another categorization of terrorist groups is determined by their level of government affiliation.

- Non-state-supported groups operate independent of government direction and receives little, if any support from foreign governments.
- State-supported groups operate independent of government control, but receives state support from one or more governments.
- State-directed groups operate as an agent of the government and receive substantial support in the form of intelligence, logistics and funding.

Army forces conduct combating terrorism operations to defeat attacks. These operations contain both offensive and defensive components. Offensive operations are counterterrorism; defensive operations are antiterrorism. The Army participates in counterterrorism operations outside the territory of the United States, while it conducts antiterrorism anywhere in the world.

## **Counter Terrorism**

Army forces participate in the full array of counterterrorism actions, including strikes and raids. Against organizations and facilities. Normally this involves special operations forces operating under a unified command arrangement. However, it may involve a commander employing conventional forces to strike against organized terrorist forces operating inside his area of operations in a combat zone.

## **Anti Terrorism**

Antiterrorism includes all defensive measures taken to reduce the vulnerability of personnel, installations, facilities, and equipment to attack. antiterrorism must be a priority of all forces on *all* operations--offensive, defensive, stability, and support. *In order to insure unit preparedness, the staff must conduct training specifically focused on the terrorist threat. The Threat Analysis and the Integrated Terrorist Threat Estimate are good tools to assess the Risk, Vulnerability and Criticality of a unit in a terrorist threat area. Staff training should be conducted IAW Ch. 5 & 17, DOD 0-2000.12-H.* Experience shows that sensational acts of terrorism against US forces can have strategic impacts. We must take great pains to protect the mission by protecting the force against terrorism.

Typical Anti-terrorism actions include:

- Coordination with local law enforcement
- Siting and hardening of facilities
- Physical security actions designed to prevent unauthorized access or approach to facilities
- Crime Prevention/Physical security actions that prevent theft of weapons, munitions, Identification cards, and other materials.
- Policies regarding travel, size of convoys, breaking routines, host -nation interaction, and 'off-duty' restrictions.

Army forces are often most vulnerable in "off-duty" periods and locations. Soldiers and families that reside outside protected installations make ideal targets to terrorist and other hostile agents. Commanders must take every effort to minimize the potential for of murders and hostage takings being used as a means to thwart stability efforts *by conducting individual antiterrorism awareness training IAW Ch. 12, DOD 0-2000.12-H and Appendix B, JP 3-07.2."*

## **Change # 10 : "Staging" section on p. V-2-12 - V-2-13:**

Paragraph Two:

"The APOD and SPOD are the most lucrative targets for enemy strikes in theater, particularly for weapons of mass destruction (WMD) *and terrorist attacks.*" These sites must be shielded from enemy conventional and unconventional attacks, normally through a combination of joint and Army assets...."



## BIBLIOGRAPHY

### Books

- Bonner, D. 1992. United Kingdom: The United Kingdom Response to Terrorism in *Terrorism: British Perspectives*, Edited by P. Wilkinson. NY: MacMillan Publishing Co.
- Callwell, C. 1990. *Small Wars: A Tactical Textbook for Imperial Soldiers*. London: Greenhill Books.
- Copher, P. and M. Monday. 1989. Hell on Wheels: Vehicle Bombs are Obviously Here to Stay. In *Security Intelligence Sourcebook*, Edited by F. McGuire. Silver Springs, Md.: Interests, Ltd.
- Crenshaw, M. 1990. The Logic of Terrorism in *Origins of Terrorism - Psychologies, Ideologies, Theologies, States of Mind*, Edited by W. Reich. NY: Cambridge Univ. Press.
- Evans, E. 1979. *Calling a Truce to Terror*. Westport, Conn.: Greenwood Press.
- Evans, E. 1987. *Wars Without Splendor*. Westport, Conn.: Greenwood Press.
- Hacker, F. J. 1977. *Crusaders, Criminals, Crazies*. NY: Norton.
- Hammel, E. 1985. *The Root: The Marines in Beirut, August 1982 - February 1984*. NY: Harcourt Brace Jovanovich, Publishers.
- Hoffer, E. 1951. *The True Believer*. NY: Harper and Row Publishers.
- Hoffman, B. And Taw, J. 1994. *A Strategic Framework for Countering Terrorism and Insurgency*. Santa Monica, Ca.: RAND Corp.
- Jenkins, M. 1985. *The Future Course of International Terrorism*. Santa Monica, Calif.: RAND Corp.
- Kitson, F. 1974. *Low Intensity Operations: Subversion, Insurgency, Peace-Keeping*. Hamden, Conn.: Archon Books.
- McKnight, G. 1974. *The Terrorist Mind*. NY: Bobbs-Merrill Co. Inc.
- McLaurin, R. and R. Miller. 1989. *Military Forces in Urban Antiterrorism*. Springfield, Va.: Abbott Associates Inc.

- Petit, M. 1986. *Peacekeepers at War*. Winchester, Ma.: Faber and Faber Inc.
- Seger, K. 1990. *The Antiterrorism Handbook*. Novato, Ca.: Presidio Press.
- Sun Tzu, *The Art of War*, Trans. Ralph D. Sawyer. Westview Press. 1994.
- Sun Tzu, *The Art of War*, Trans. Samuel B. Griffith. Oxford University Press. 1963.
- Vetter, H. J., and G.R. Perlstein. 1991. *Perspectives on Terrorism*. Belmont, Calif.: Brooks/Cole Publishing Co.
- Von Clausewitz, Carl. *On War* Trans. Michael Howard and Peter Paret. Princeton: Princeton University Press. 1976
- Vought, D. 1993. The Coming Age of Terror. In *Security Intelligence Sourcebook*. Edited by F. McGuire. Silver Spring, Md.: Interests, Ltd.
- Wardlaw, G. 1989. *Political Terrorism*. NY: Cambridge Univ. Press.

#### Government Publications

- Chairman, Joint Chiefs of Staff. Pub 1-02. *Department of Defense Dictionary of Military and Associated Terms*. Washington, DC: 1994.
- Chairman, Joint Chiefs of Staff. Pub 3-0. *Doctrine for Joint Operations*. Washington, DC: 1995.
- Chairman, Joint Chiefs of Staff. Pub 3-07.2. *Joint Tactics, Techniques, and Procedures for Antiterrorism*. Washington, DC: 1993.
- Department of Defense. Directive 0-2000.12. *Combating Terrorism Program*. Washington, DC: Department of Defense, 1996.
- Department of Defense. Directive 0-2000.12-H. *Protection of DOD Personnel and Activities Against Acts of Terrorism and Public Turbulence*. Washington, DC: Department of Defense, 1993.
- Department of the Army. Regulation 190-58. *Personal Security*. Washington, DC: Headquarters, Department of the Army, 1989.
- Department of the Army. Regulation 381-12. *Subversion and Espionage Directed Against the U. S. Army (SAEDA)*. Washington, DC: Headquarters, Department of the Army, 1993.

- Department of the Army. Regulation 525-13. *The Army Combating Terrorism Program*. Washington, DC: Headquarters, Department of the Army, 1992.
- Department of the Army. Field Manual 100-5. *Operations*. Washington, DC: Headquarters, Department of the Army, 1993.
- Department of the Army. Field Manual 100-5 (Coordinating Draft). *Operations*. Leavenworth, Ks: Combined Arms Center, 14 January 1997.
- Secretary of Defense Report to the President. 16 September 1996. *Force Protection: Global Interest, Global Responsibilities*.
- Secretary of Defense. 9 July 1996. Prepared Statement of William J. Perry, Secretary of Defense, before the Senate Armed Services Committee in Connection with The Saudi Arabia Bombing. Federal Info Systems Corp. Transcript 961910088.
- United States Army Training and Doctrine Command. Pamphlet 525-71. 1996. *Force XXI Division Operations Concept*. Ft. Monroe, Va.: United States Army Training and Doctrine Command.
- United States Government, "Report of the DOD Commission on Beirut International Airport Terrorist Act, October 23, 1983". 20 December 1983.
- United States Marine Corps. FMFM 7-14 *Combating Terrorism*. Washington, DC: Department of the Navy, 1990.
- United States Marine Corps. FMFRP 7-14A *Individual's Guide for Understanding and Surviving Terrorism*. Washington, DC: Department of the Navy, 1989.
- United States Government, "Force Protection Assessment of USCENTCOM AOR and Khobar Towers: Report of the Downing Assessment Task Force"(Unclassified). 30 August 1996.

#### Periodicals

- Bombs in the Desert. 1996. *U. S. News & World Report*, 07 August.
- Telling Friend From Foe. 1995. *U.S. News & World Report*, 27 November.

### Newspapers

Graham, B. 1996. Perry Accepts Blame In Dhahran Bombing. *Washington Post*, 19 September.

Pentagon Negligence. 1996. *New York Times*, 18 September, A 20.

Shenon, P. 1996. United States and Saudis Agree to Split Cost of Safeguarding G.I.'s. *New York Times*, 1 August.